

**IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF TENNESSEE**

IN RE: COMMUNITY HEALTH  
SYSTEMS, INC. DATA SECURITY  
LITIGATION

This Document Relates To:  
ALL ACTIONS

MASTER FILE NO. 3:23-cv-00285

Chief Judge Waverly D. Crenshaw, Jr.  
Magistrate Judge Alistair Newbern

**CLASS ACTION**

**JURY DEMAND**

**CONSOLIDATED AMENDED CLASS ACTION COMPLAINT**

**SANFORD HEISLER SHARP, LLP**

Kevin H. Sharp, BPR No. 016287  
Leigh Anne St. Charles, BPR No. 036945  
Jonathan Tepe, BPR No. 037266  
611 Commerce Street, Suite 3100  
Nashville, TN 37203  
Telephone: (615) 434-7000  
Facsimile: (615) 434-7020  
ksharp@sanfordheisler.com  
lstcharles@sanfordheisler.com  
jtepe@sanfordheisler.com

**BARNOW AND ASSOCIATES, P.C.**

Ben Barnow (admitted *pro hac vice*)  
Anthony L. Parkhill (admitted *pro hac vice*)  
Riley W. Prince (admitted *pro hac vice*)  
205 West Randolph Street, Ste. 1630  
Chicago, IL 60606  
Tel: 312-621-2000  
Fax: 312-641-5504  
b.barnow@barnowlaw.com  
aparkhill@barnowlaw.com  
rprince@barnowlaw.com

**SHUB & JOHNS LLC**

Benjamin F. Johns (admitted *pro hac vice*)  
Samantha E. Holbrook (admitted *pro hac vice*)  
Four Tower Bridge  
200 Barr Harbor Drive, Suite 400  
Conshohocken, PA 19428  
(610) 477-8380  
bjohns@shublawyers.com  
sholbrook@shublawyers.com

**BAILEY GLASSER LLP**

Bart D. Cohen (admitted *pro hac vice*)  
1622 Locust Street  
Philadelphia, PA 19103  
(215) 274-9420  
bcohen@baileyglasser.com

*Interim Co-Lead Class Counsel*

## TABLE OF CONTENTS

INTRODUCTION .....	1
PARTIES.....	3
JURISDICTION AND VENUE .....	12
FACTUAL ALLEGATIONS .....	12
CLASS ALLEGATIONS.....	26
CAUSES OF ACTION.....	29
COUNT I .....	29
NEGLIGENCE (Against Both Defendants On Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes) .....	29
COUNT II.....	32
NEGLIGENCE <i>PER SE</i> (Against Both Defendants On Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes) .....	32
COUNT III .....	34
BREACH OF FIDUCIARY DUTY (Against Both Defendants on Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes) .....	34
COUNT IV .....	35
BREACH OF IMPLIED CONTRACT (Against Both Defendants on Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes) .....	35
COUNT V .....	38
BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS WERE INTENDED THIRD PARTY BENEFICIARIES (Against Both Defendants on Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes).....	38
COUNT VI .....	39
UNJUST ENRICHMENT(Against Both Defendants on Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes) .....	39
COUNT VII.....	40
VIOLATIONS OF ALABAMA DECEPTIVE TRADE PRACTICES ACT Ala. Code § 8-19-1, <i>et seq.</i> (Against Both Defendants on Behalf of the Alabama Class).....	40
COUNT VIII.....	42

VIOLATIONS OF MISSISSIPPI DECEPTIVE TRADE PRACTICES ACT Miss. Code § 75-24-1, <i>et seq.</i> (Against Both Defendants on Behalf of the Mississippi Class) .....	42
COUNT IX .....	44
VIOLATIONS OF PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW 73 Pa. Stat. Ann. § 201-1, <i>et seq</i> (Against Both Defendants on Behalf of the Pennsylvania Class).....	44
COUNT X .....	46
VIOLATIONS OF TENNESSEE CONSUMER PROTECTION ACT Tenn. Code Ann. § 47-18-101, <i>et seq</i> (Against Both Defendants on Behalf of the Tennessee Class).....	46
PRAYER FOR RELIEF .....	49
JURY TRIAL DEMANDED.....	49

Plaintiffs Sandra Kuffrey, Angela Martin, Lola Tatum, Richard Walck, Glenda G. Corn, Wilhelmina Gill, Brandy McGowen, and Kelly Kern, individually, and on behalf of all others similarly situated (collectively, “Class members”), by and through their attorneys, bring this Consolidated Amended Class Action Complaint against Defendants Community Health Systems, Inc. (“CHS”), and CHSPSC, LLC (“CHSPSC”) (collectively, “Defendants”) and complain and allege upon personal knowledge as to themselves, and information and belief as to all other matters.

## **INTRODUCTION**

1. Plaintiffs bring this class action against Defendants for their failure to secure and safeguard their and approximately 1,173,555 other individuals’ personally identifying information (“PII”) and personal health information (“PHI”), including names, dates of birth, addresses, medical billing and insurance information, medical diagnoses, prescription information, and Social Security numbers.

2. Defendant CHS is one of the largest publicly traded hospital companies in the United States.<sup>1</sup> Defendant CHSPSC is a related entity that provides “management services” for entities affiliated with CHS.<sup>2</sup> Specifically, CHSPSC identifies and enters into contracts with vendors to provide services for CHS and its affiliates. CHS’s website states that “we . . . hold CHSPSC and CHS affiliated entities’ vendors and their representatives to specific standards of conduct when committing financial resources for the purchase of goods, services, and equipment.”<sup>3</sup>

---

<sup>1</sup> <https://www.chs.net/company-overview/> (last accessed June 9, 2023).

<sup>2</sup> <https://www.chs.net/company-overview/vendor-information/> (last accessed June 9, 2023).

<sup>3</sup> *Id.*

3. On February 2, 2023, CHSPSC was notified that one of the vendors with which it had contracted —Fortra, LLC (“Fortra”), the provider of a file transfer software used by CHSPSC —experienced a data breach between January 28, 2023 and January 30, 2023. Unauthorized individual(s) breached Fortra’s network systems and accessed and acquired files containing the PII and PHI of Defendants’ and their affiliates’ patients and employees, including Plaintiffs and Class members (the “Data Breach”).

4. CHS and CHSPSC owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. They breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their patients’ and employees’ PII/PHI from unauthorized access and disclosure.

5. As a result of Defendants’ inadequate vendor screening, inadequate security measures, and breach of their legal duties and obligations, the Data Breach occurred, and Plaintiffs’ and Class members’ PII/PHI was accessed and disclosed. Their failure to reasonably safeguard this information was also contrary to statements made in their own “Code of Conduct,” as discussed in more detail below. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose PII/PHI was exposed as a result of the Data Breach.

6. The Data Breach was reasonably foreseeable to Defendants. In fact, CHS was the subject of a massive breach in 2014 that impacted 6.1 million patients. On September 22, 2020, both CHSPSC and CHS entered into a consent decree with the Iowa Attorney General and 27 other participating states whereby they agreed to pay \$5 million to resolve allegations that they lacked

sufficient security measures in relation to the 2014 breach.<sup>4</sup> CHSPSC and CHS also agreed to settle a similar investigation with the HHS' Office for Civil Rights for \$2.3 million, as well as a class action lawsuit for \$3.1 million.<sup>5</sup>

7. Plaintiffs, on behalf of themselves and all other Class members, assert claims herein concerning the Data Breach at CHS and CHSPSC for negligence, negligence *per se*, breach of fiduciary duty, breach of implied contract, breach of contracts to which Plaintiffs and Class Members are intended third party beneficiaries, violations of state statutes, unjust enrichment, and violations of several state consumer fraud statutes. They seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

## **PARTIES**

### ***Plaintiff Sandra Kuffrey***

8. Plaintiff Sandra Kuffrey is a citizen of Tennessee.

9. Plaintiff Kuffrey was employed by Tennova Healthcare – Cleveland, an affiliate of Defendants, and obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants. As a condition of her employment and receiving these services, Defendants required her to provide Defendants with her PII/PHI.

10. Based on representations made by Defendants, Plaintiff Kuffrey believed that they had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff Kuffrey provided her PII/PHI to Defendants as a condition of her

---

<sup>4</sup>[https://www.iowaattorneygeneral.gov/media/cms/CHS\\_Consent\\_Decree\\_4FD176209906F.PDF](https://www.iowaattorneygeneral.gov/media/cms/CHS_Consent_Decree_4FD176209906F.PDF) (last accessed June 9, 2023).

<sup>5</sup><https://www.hipaajournal.com/community-health-systems-pays-5-million-to-settle-multi-state-breach-investigation/> (last accessed June 9, 2023).

employment, and in connection with and in exchange for receiving healthcare or related services from Defendants.

11. In connection with her employment and services provided to Plaintiff Kuffrey, Defendants store and maintain Plaintiff Kuffrey PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

12. Plaintiff Kuffrey takes great care to protect her PII/PHI. Had Plaintiff Kuffrey known that Defendants do not adequately protect the PII/PHI in their possession, she would not have obtained or used services from Defendants or agreed to provide Defendants with her PII/PHI.

13. In a letter addressed to Plaintiff Kuffrey, Defendant CHSPSC, LLC disclosed to Ms. Kuffrey that her PII and/or PHI was accessible as a result of the Data Breach.

14. As a direct result of the Data Breach, Plaintiff Kuffrey has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

***Plaintiff Angela Martin***

15. Plaintiff Angela Martin is a citizen of Alabama.

16. Plaintiff Martin obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants. As a condition of receiving these services, Defendants required her to provide them with her PII/PHI.

17. Based on representations made by Defendants, Plaintiff Martin believed that they had implemented and maintained reasonable security and practices to protect her PII/PHI. With

this belief in mind, Plaintiff Martin provided her PII/PHI to Defendants in connection with and in exchange for receiving healthcare or related services from Defendants.

18. In connection with services provided to Plaintiff Martin, Defendants store and maintain Plaintiff Martin's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

19. Plaintiff Martin takes great care to protect her PII/PHI. Had Plaintiff Martin known that Defendants do not adequately protect the PII/PHI in their possession, she would not have obtained or used services from Defendants or agreed to provide Defendants with her PII/PHI.

20. In a letter addressed to Plaintiff Martin, defendant CHSPSC, LLC disclosed to Plaintiff Martin that her PII and/or PHI was accessible as a result of the Data Breach.

21. Plaintiff Martin has experienced fraud since cybercriminals obtained her PII/PHI in the Data Breach. An unauthorized person or persons attempted to open a Zelle account in her name. She has also received alerts that people are applying for other bank accounts. Also, in late January or early February of 2023, she had two attempted unauthorized transactions made on her bank account. She has also been advised by Experian that her personal information is now on the dark web. Ms. Martin estimates that she has spent approximately 40 hours dealing with these issues.

22. As a direct result of the Data Breach, Plaintiff Martin has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.



***Plaintiff Lola Tatum***

23. Plaintiff Lola Tatum is a citizen of Mississippi.

24. Plaintiff Tatum obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants.

25. Plaintiff Tatum was previously employed by an affiliate of Defendants.

26. As a condition of receiving healthcare or related services, and in connection with her employment, Defendants required Plaintiff Tatum to provide Defendants with her PII/PHI.

27. Based on representations made by Defendants, Plaintiff Tatum believed that Defendants had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff Tatum provided her PII/PHI to Defendants in connection with her employment and in exchange for receiving healthcare or related services from Defendants.

28. In connection with employment and services provided to Plaintiff Tatum, Defendants store and maintain Plaintiff Tatum's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

29. Plaintiff Tatum takes great care to protect her PII/PHI, including her Medicare information. Had Plaintiff Tatum known that Defendants do not adequately protect the PII/PHI in their possession, she would not have obtained or used services or employment from Defendants or their affiliates or agreed to provide Defendants with her PII/PHI.

30. 37. In a letter addressed to Plaintiff Tatum, Defendant CHSPSC, LLC disclosed to Plaintiff Tatum that her PII and/or PHI was accessible as a result of the Data Breach.

31. As a direct result of the Data Breach, Plaintiff Tatum has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity

theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

***Plaintiff Richard Walck***

32. Plaintiff Richard Walck is a citizen of Mississippi.

33. Plaintiff Walck obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants. As a condition of receiving these services, Defendants required Plaintiff Walck to provide Defendants with his PII/PHI.

34. Based on representations made by Defendants, Plaintiff Walck believed that Defendants had implemented and maintained reasonable security and practices to protect his PII/PHI. With this belief in mind, Plaintiff Walck provided his PII/PHI to Defendants in connection with and in exchange for receiving healthcare or related services from Defendants.

35. In connection with services provided to Plaintiff Walck, Defendants store and maintain Plaintiff Walck's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

36. Plaintiff Walck takes great care to protect his PII/PHI. Had Plaintiff Walck known that Defendants do not adequately protect the PII/PHI in their possession, he would not have obtained or used services from Defendants or agreed to provide Defendants with his PII/PHI.

37. In a letter addressed to Plaintiff Walck, Defendant CHSPSC, LLC disclosed to Plaintiff Walck that his PII and/or PHI was accessible as a result of the Data Breach.

38. As a direct result of the Data Breach, Plaintiff Walck has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI;

deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

***Plaintiff Glenda G. Corn***

39. Plaintiff Glenda G. Corn is a citizen of Florida.

40. Plaintiff Corn obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants. As a condition of receiving these services, Defendants required Plaintiff Corn to provide Defendants with her PII/PHI.

41. Based on representations made by Defendants, Plaintiff Corn believed that Defendants had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff Corn provided her PII/PHI to Defendants in connection with and in exchange for receiving healthcare or related services from Defendants.

42. In connection with services provided to Plaintiff Corn, Defendants store and maintain Plaintiff Corn's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

43. Plaintiff Corn takes great care to protect her PII/PHI. Had Plaintiff Corn known that Defendants do not adequately protect the PII/PHI in their possession, she would not have obtained or used services from Defendants or their affiliates or agreed to provide Defendants with her PII/PHI.

44. In a letter addressed to Plaintiff Corn, Defendant CHSPSC, LLC disclosed to Plaintiff Corn that her PII and/or PHI was accessible as a result of the Data Breach

45. As a direct result of the Data Breach, Plaintiff Corn has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft;

the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

***Plaintiff Wilhelmina Gill***

46. Plaintiff Wilhelmina Gill is a citizen of Tennessee.

47. Plaintiff Gill obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants. As a condition of receiving these services, Defendants required Plaintiff Gill to provide Defendants with her PII/PHI.

48. Based on representations made by Defendants, Plaintiff Gill believed that Defendants had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff Gill provided her PII/PHI to Defendants in connection with and in exchange for receiving healthcare or related services from Defendants.

49. In connection with services provided to Plaintiff Gill, Defendants store and maintain Plaintiff Gill PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

50. Plaintiff Gill takes great care to protect her PII/PHI. Had Plaintiff Gill known that Defendants do not adequately protect the PII/PHI in their possession, she would not have obtained or used services from Defendants or their affiliates or agreed to provide Defendants with her PII/PHI.

51. In a letter addressed to Plaintiff Gill, Defendant CHSPSC, LLC disclosed to Plaintiff Gill that her PII and/or PHI was accessible as a result of the Data Breach

52. As a direct result of the Data Breach, Plaintiff Gill has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft;

the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

***Plaintiff Kelly Kern***

53. Plaintiff Kelly Kern is a citizen of Pennsylvania.

54. Plaintiff Kern obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants. As a condition of receiving these services, Defendants required Plaintiff Kern to provide Defendants with her PII/PHI.

55. Based on representations made by Defendants, Plaintiff Kern believed that Defendants had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff Kern provided her PII/PHI to Defendants in connection with and in exchange for receiving healthcare or related services from Defendants.

56. In connection with services provided to Plaintiff Kern, Defendants store and maintain Plaintiff Kern's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

57. Plaintiff Kern takes great care to protect her PII/PHI. Had Plaintiff Kern known that Defendants do not adequately protect the PII/PHI in its possession, she would not have obtained or used services from Defendants or agreed to provide Defendants with her PII/PHI.

58. In a letter addressed to Plaintiff Kern, Defendant CHSPSC, LLC disclosed to Plaintiff Kern that her PII and/or PHI was accessible as a result of the Data Breach.

59. Plaintiff Kern has experienced suspicious activity subsequent to the Data Breach. On April 13, 2023, she received a text message from Fidelity Bank asking to confirm an \$85 purchase that was made in another state. This was the first time Plaintiff Kern had ever experienced an issue like this.

60. As a direct result of the Data Breach, Plaintiff Kern has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

***Plaintiff Brandy McGowen***

61. Plaintiff Brandy McGowen is a citizen of Mississippi.

62. Plaintiff McGowen obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants. As a condition of receiving these services, Defendants required Plaintiff McGowen to provide Defendants with her PII/PHI.

63. Based on representations made by Defendants, Plaintiff McGowen believed that Defendants had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff McGowen provided her PII/PHI to Defendants in connection with and in exchange for receiving healthcare or related services from Defendants.

64. In connection with services provided to Plaintiff McGowen, Defendants store and maintain Plaintiff McGowen's PII/PHI on their systems and transmitted the PII/PHI to third parties, including Fortra.

65. Plaintiff McGowen takes great care to protect her PII/PHI. Had Plaintiff McGowen known that Defendants do not adequately protect the PII/PHI in its possession, she would not have obtained or used services from Defendants or agreed to provide Defendants with her PII/PHI.

66. In a letter addressed to Plaintiff McGowen, Defendant CHSPSC, LLC disclosed to Plaintiff McGowen that her PII and/or PHI was accessible as a result of the Data Breach.

67. As a direct result of the Data Breach, Plaintiff McGowen has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity

theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

### ***Defendants***

68. Defendant CHSPSC, LLC is a Delaware corporation with its principal place of business in Franklin, Tennessee. CHSPSC's headquarters are located at 4000 Meridian Blvd., Franklin, Tennessee 37067.

69. Defendant Community Health Systems, Inc. is a Delaware corporation, with its principal place of business in Franklin, Tennessee.

### **JURISDICTION AND VENUE**

70. The Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from CHSPSC, and (c) the matter in controversy exceeds \$5,000,000, exclusive of interest and costs.

71. This Court has personal jurisdiction over Defendants because they both maintain their principal place of business in Tennessee.

72. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because CHSPSC's principal place of business is in this District and a significant amount of the events leading to Plaintiffs' causes of action occurred in this District.

### **FACTUAL ALLEGATIONS**

#### ***Overview of CHSPSC and CHS***

73. "CHSPSC is a professional services company that provides services to hospitals

and clinics affiliated with Community Health Systems, Inc.”<sup>6</sup> Upon information and belief, CHSPSC is a subsidiary of CHS.

74. CHS is a publicly traded company whose stock (CYH) has been listed on the New York Stock Exchange since 2000. In its Form 10-K filed with the Securities and Exchange Commission for the year ended 2022, CHS reported \$12.2 billion in revenue, with \$1.4 billion in earnings before interest, taxes, depreciation, and amortization.

75. CHS describes itself as “one of the nation’s leading healthcare providers.”<sup>7</sup> It operates in 15 states: Alabama, Alaska, Arizona, Arkansas, Florida, Georgia, Indiana, Mississippi, Missouri, New Mexico, North Carolina, Oklahoma, Pennsylvania, Tennessee and Texas.<sup>8</sup> It maintains 78 acute-care hospitals and more than 1,000 other sites of care, including physician practices, urgent care centers, freestanding emergency departments, occupational medicine clinics, imaging centers, cancer centers, and ambulatory surgery centers.<sup>9</sup>

76. Due to the nature of the services that they provide, CHSPSC and CHS acquire and electronically store patient PII and PHI: “When a patient enters a CHS affiliated facility, a large amount of personal, medical, and insurance data is collected.”<sup>10</sup> The Defendants’ Code of Conduct states “[p]atient information may only be discussed or released as permitted or required under the Health Insurance Portability and Accountability Act (‘HIPAA’) or other privacy laws and in

---

<sup>6</sup> *Notice of Third-Party Security Incident Impacting CHSPSC Affiliate Data* (“Website Notice”), CMTY. HEALTH SYS., <https://www.chs.net/notice-of-third-party-security-incident-impacting-chspsc-affiliate-data/> (last accessed June 15, 2023).

<sup>7</sup> <https://www.chs.net/> (last accessed June 8, 2023).

<sup>8</sup> *Locations*, CMTY. HEALTH SYS., <https://www.chs.net/serving-communities/locations/#USMap> (last accessed Apr. 26, 2023).

<sup>9</sup> *Id.*

<sup>10</sup> Community Health Systems, *Community Health Systems Code of Conduct*, at 9 (2023), <https://www.chs.net/wp-content/uploads/Code-of-Conduct-January-2023-FINAL.pdf>. The Code of Conduct applies to, and has been independently adopted by, each subsidiary of Community Health Systems, including CHSPSC. *See id.*



accordance with our HIPAA policies . . . which may require either a patient-directed request, a request from a patient's personal representative, or the express written authorization of the patient.”<sup>11</sup>

77. The Defendants' Code of Conduct also states that they are “dedicated to compliance with all applicable federal, state, and local laws, rules, and regulations (‘Applicable Law’), including privacy and security of patient health information.”<sup>12</sup> And Defendants acknowledge that “[p]atient information is highly confidential.”<sup>13</sup> CHSPSC also states patient rights include “[p]ersonal privacy” and “privacy of health information.”<sup>14</sup>

### ***The 2014 Data Breach***

78. As noted above, CHS and CHSPSC were previously the target of a data breach that compromised the sensitive personal information of over six million people. The hackers, who were believed to be based in China, were able to gain access to Defendants' internal computer systems between April and June 2014. The data that was exfiltrated included patient names, Social Security numbers, addresses, dates of birth, and phone numbers.

79. Shortly after this breach was announced, the Iowa Attorney General filed a complaint against CHS and CHSPSC which alleged, *inter alia*, that Defendants:

- A. Failed to implement and maintain reasonable security practices to protect consumers' personal information they collect and maintain;
- B. Failed to store personal information in a way that maximized its security and confidentiality; and

---

<sup>11</sup> *Id.* at 10.

<sup>12</sup> *Id.* at 3.

<sup>13</sup> *Id.* at 9.

<sup>14</sup> *Id.* at 11.

C. Permitted the disclosure of Protected Health Information in a manner inconsistent with the requirements of HIPAA and its rules.<sup>15</sup>

80. Several other Attorneys General also prosecuted similar claims against Defendants. These matters were resolved in 2020 for \$5 million. Iowa Attorney General Tom Miller issued a statement at that time that said “CHS failed to implement and maintain reasonable security practices.”<sup>16</sup>

81. CHSPSC agreed to pay another \$2.3 million to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) in connection with the 2014 breach.<sup>17</sup>

A statement issued by this agency announcing the settlement stated that its

investigation found longstanding, systemic noncompliance with the HIPAA Security Rule including failure to conduct a risk analysis, and failures to implement information system activity review, security incident procedures, and access controls. “The health care industry is a known target for hackers and cyberthieves. The failure to implement the security protections required by the HIPAA Rules, especially after being notified by the FBI of a potential breach, is inexcusable,” said OCR Director Roger Severino.<sup>18</sup>

82. CHS additionally agreed to settle a class action lawsuit filed in connection with the 2014 data breach for \$3.1 million.<sup>19</sup>

### ***The 2023 Data Breach***

83. Defendants contracted with Fortra, a company that sells information technology

---

<sup>15</sup> [https://www.iowaattorneygeneral.gov/media/cms/CHS\\_Petition\\_011932DDEE45E.pdf](https://www.iowaattorneygeneral.gov/media/cms/CHS_Petition_011932DDEE45E.pdf) (last accessed June 9, 2023).

<sup>16</sup> <https://www.fiercehealthcare.com/tech/chs-to-pay-5m-to-28-states-to-settle-2014-data-breach> (last accessed June 9, 2023).

<sup>17</sup> <https://public3.pagefreezer.com/content/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/about/news/2020/09/23/hipaa-business-associate-pays-2.3-million-settle-breach.html> (last accessed June 9, 2023).

<sup>18</sup> *Id.*

<sup>19</sup> <https://cyware.com/news/community-health-systems-agrees-to-pay-nearly-31-million-as-a-part-of-settlement-for-2014-data-breach-73d4c448> (last accessed June 9, 2023).

management software and services, for the use of file transfer software called “GoAnywhere.”<sup>20</sup> Defendants upload, store, transfer, or access their or their affiliates’ patients’ and employees’ PII/PHI using GoAnywhere.

84. Between January 28 and January 30, 2023, an unauthorized individual or individuals “used a previously unknown vulnerability to gain access to Fortra’s systems, specifically Fortra’s GoAnywhere file transfer service platform, compromising sets of files throughout Fortra’s platform.”<sup>21</sup>

85. Fortra first notified Defendants of the Data Breach on February 2, 2023.<sup>22</sup> The Defendants then undertook their own investigation, which revealed that the personal information of patients, employees, and other individuals “may have been disclosed to the unauthorized party as a result of the Fortra incident.”<sup>23</sup> Specifically, the compromised data may have included full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and Social Security number.<sup>24</sup>

86. CHS has acknowledged in its SEC filings that the compromised information included “Protected Health Information” as defined by HIPAA.<sup>25</sup>

87. The Data Breach impacted the PII/PHI of certain persons who received services from Defendants or their affiliates, family members or guarantors of patients of Defendants or their

---

<sup>20</sup> See Website Notice, *supra*, n.6.

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

<sup>23</sup> *Id.*

<sup>24</sup> *Id.*

<sup>25</sup> <https://chsnet.gcs-web.com/static-files/706bf25d-a064-4a04-90b6-bf4e5357defa> (last accessed June 15, 2023).

affiliates, and current or former employees of Defendants or their affiliates.<sup>26</sup>

88. CHSPSC began notifying affected persons on or around March 20, 2023.<sup>27</sup> CHSPSC's Website Notice states that it has "implemented additional security measures, including immediate steps to implement measures to harden the security of CHSPSC's use of the GoAnywhere platform."<sup>28</sup>

89. The CHS and CHSPSC patient data compromised in the Data Breach was reportedly intentionally targeted by a criminal ransomware group linked to Russia and known as Clop.<sup>29</sup> It has not been reported whether Defendants were solicited to pay or actually paid a ransom demand.

90. In a press release issued on May 16, 2023 discussing the various organizations that were targeted in the Data Breach, Michigan Attorney General Dana Nessel said "[c]ompanies that handle our personal data have a responsibility to implement safety measures that can withstand cyber-attacks. . . A breach like this one threatens to expose some of our most personal information – our health information."<sup>30</sup>

#### ***CHSPSC Knew that Criminals Target PII/PHI***

91. At all relevant times, Defendants knew, or should have known, that the PII/PHI that they collected was a target for malicious actors. Indeed, CHS notes:

A cyber-attack or security breach could result in the compromise of our facilities, confidential data or critical data systems and give rise to potential harm to patients, remediation and other expenses, expose us to liability under HIPAA, privacy and data protection laws and regulations, consumer protection laws, common law or

---

<sup>26</sup> *Id.*

<sup>27</sup> See *CHSPSC, LLC Data Breach Notification*, ME. ATT'Y GEN., <https://apps.web.maine.gov/online/aewviewer/ME/40/e71fd844-b34a-449c-aba9-e4f63265f422.shtml> (last accessed June 14, 2023).

<sup>28</sup> *Id.*

<sup>29</sup> <https://techcrunch.com/2023/02/15/clop-ransomware-community-health-systems/> (last accessed June 8, 2023).

<sup>30</sup> <https://www.michigan.gov/ag/news/press-releases/2023/05/16/fortra-data-breach-targets-130-companies-many-in-healthcare-sector> (last accessed June 14, 2023).

other theories, subject us to litigation and federal and state governmental inquiries, damage our reputation, and otherwise be disruptive to our business.<sup>31</sup>

CHS further admits:

[T]here can be no assurance that we, or our third-party vendors and providers, will not be subject to security breaches and other cybersecurity threats, including those related to the use of ransomware and other malicious software or other attempts by third parties to access, acquire, use, disclose, misappropriate or manipulate our information or disrupt our operations.<sup>32</sup>

92. CHS recognizes “the volume and intensity of cyber-attacks on hospitals and health systems continues to increase,” and admits it is “regularly the target of attempted cybersecurity and other threats that could have a security impact, and [it] expect[s] to continue to experience an increase in cybersecurity threats in the future.”<sup>33</sup>

93. CHS states, “We may be at increased risk because we outsource certain services or functions to, or have systems that interface with, third parties. Some of these third parties’ information systems are also subject to [cyber-security] risks . . . and may store or have access to our data and may not have effective controls, processes, or practices to protect our information from attack, damage, or unauthorized access, acquisition, use or disclosure.”<sup>34</sup>

94. CHS knew that “[i]f [it] or any of [its] third-party service providers or certain other third-parties are subject to cyber-attacks or security or data breaches in the future, this could result in harm to patients . . . [and] the loss, misappropriation, corruption or unauthorized access, acquisition, use or disclosure of data.”<sup>35</sup>

---

<sup>31</sup> Community Health Systems, *Form 10K* 42 (2022), <https://chsnet.gcs-web.com/static-files/6a50aed5-21f9-474d-856c-d4fb8e595eab>.

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*

<sup>34</sup> *Id.* at 43.

<sup>35</sup> *Id.*

95. Thus, Defendants knew or should have known of these risks. Despite such knowledge, they both failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs’ and Class members’ PII/PHI from cyber-attacks that Defendants should have anticipated and guarded against.

96. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers (“SSNs”) and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that “[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores.”<sup>36</sup>

97. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.<sup>37</sup> This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.<sup>38</sup>

---

<sup>36</sup> Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.), <https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1>.

<sup>37</sup> See PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, <https://www.protenus.com/breach-barometer-report> (last accessed Apr. 26, 2023).

<sup>38</sup> See *id.*

98. PII/PHI is a valuable property right.<sup>39</sup> The value of PII/PHI as a commodity is measurable.<sup>40</sup> “Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks.”<sup>41</sup> American companies are estimated to have spent over \$19 billion on acquiring personal data of consumers in 2018.<sup>42</sup> It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the “cyber black-market,” or the “dark web,” for many years.

99. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

---

<sup>39</sup> See Marc van Lieshout, *The Value of Personal Data*, 457 INT’L FED’N FOR INFO. PROCESSING 26 (May 2015) (“The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...”), [https://www.researchgate.net/publication/283668023\\_The\\_Value\\_of\\_Personal\\_Data](https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data).

<sup>40</sup> See Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for \$50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), <http://www.medscape.com/viewarticle/824192>.

<sup>41</sup> OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), [https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data\\_5k486qtxldmq-en](https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en).

<sup>42</sup> See IAB Data Center of Excellence, *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), <https://www.iab.com/news/2018-state-of-data-report/>.

100. PHI is particularly valuable and has been referred to as a “treasure trove for criminals.”<sup>43</sup> A cybercriminal who steals a person’s PHI can end up with as many as “seven to ten personal identifying characteristics of an individual.”<sup>44</sup>

101. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to \$1,200 to \$1,300 each on the black market.<sup>45</sup> According to a report released by the Federal Bureau of Investigation’s (“FBI”) Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.<sup>46</sup>

102. Criminals can use stolen PII/PHI to extort a financial payment by “leveraging details specific to a disease or terminal illness.”<sup>47</sup> Quoting Carbon Black’s Chief Cybersecurity Officer, one recent article explained: “Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do.”<sup>48</sup>

---

<sup>43</sup> See Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon> (“*What Happens to Stolen Healthcare Data*”) (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating “Health information is a treasure trove for criminals.”).

<sup>44</sup> *Id.*

<sup>45</sup> See SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), <https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market>.

<sup>46</sup> See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), <https://www.illumweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf>.

<sup>47</sup> *What Happens to Stolen Healthcare Data*, *supra* note 43.

<sup>48</sup> *Id.*



103. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”<sup>49</sup>

104. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers’ PII/PHI has thus deprived that consumer of the full monetary value of the consumer’s transaction with the company.

***Theft of PII/PHI Has Grave and Lasting Consequences for Victims***

105. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person’s name.<sup>50</sup>

106. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.<sup>51</sup> Experian, one of the largest credit reporting companies in the world, warns consumers that “[i]dentity thieves can profit off your personal information” by, among other things, selling the information, taking over accounts, using

---

<sup>49</sup> Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) <https://www.jstor.org/stable/23015560?seq=1>.

<sup>50</sup> See Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM’N CONSUMER INFO., <https://www.consumer.ftc.gov/articles/what-know-about-identity-theft> (last accessed Apr. 26, 2023).

<sup>51</sup> The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 12 C.F.R. § 1022.3(h). The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” 12 C.F.R. § 1022.3(g).

accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.<sup>52</sup>

107. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.<sup>53</sup>

108. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.<sup>54</sup>

109. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

110. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to

---

<sup>52</sup> See Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

<sup>53</sup> See Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last accessed Apr. 26, 2023).

<sup>54</sup> See Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2021), <https://www.idtheftcenter.org/identity-theft-aftermath-study/> (last accessed Apr. 26, 2022).

find flaws in their computer systems, as stating, “If I have your name and your Social Security number and you don’t have a credit freeze yet, you’re easy pickings.”<sup>55</sup>

111. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information “typically leave[] a trail of falsified information in medical records that can plague victims’ medical and financial lives for years.”<sup>56</sup> It “is also more difficult to detect, taking almost twice as long as normal identity theft.”<sup>57</sup> In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI “to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care.”<sup>58</sup> The FTC also warns, “If the thief’s health information is mixed with yours it could affect the medical care you’re able to get or the health insurance benefits you’re able to use.”<sup>59</sup>

112. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services neither sought nor received.

---

<sup>55</sup> Patrick Lucas Austin, *‘It Is Absurd.’ Data Breaches Show it’s Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), <https://time.com/5643643/capital-one-equifax-data-breach-social-security/>.

<sup>56</sup> Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), [http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF\\_Geography\\_of\\_Medical\\_Identity\\_Theft\\_fs.pdf](http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf).

<sup>57</sup> See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk...*, *supra* note 46.

<sup>58</sup> See *What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, <https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last accessed Apr. 26, 2023).

<sup>59</sup> *Id.*

- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.<sup>60</sup>

113. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.<sup>61</sup>

114. It is within this context that Plaintiffs and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by and in the possession of people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

---

<sup>60</sup> See Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* note 56.

<sup>61</sup> John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), <http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf>.

### ***Damages Sustained by Plaintiffs and the Other Class Members***

115. Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) loss of value of their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

### **CLASS ALLEGATIONS**

116. This action is brought and may be properly maintained as a class action pursuant to Rules 23(a), 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure.

117. Plaintiffs bring this action on behalf of themselves and all members of the following Nationwide Class of similarly situated persons:

All persons in the United States and its territories whose personally identifiable information or personal health information was compromised in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

118. In the alternative to the Nationwide Class, Plaintiffs seek to represent each of the following state-wide classes (the Nationwide Class and State-Wide Classes are collectively referred to as the "Class"):

**Alabama Class:** All persons in Alabama whose personally identifiable information or personal health information was compromised in the Data Breach by

unauthorized persons, including all persons who were sent a notice of the Data Breach.

**Florida Class:** All persons in Florida whose personally identifiable information or personal health information was compromised in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

**Mississippi Class:** All persons in Mississippi whose personally identifiable information or personal health information was compromised in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

**Pennsylvania Class:** All persons in Pennsylvania whose personally identifiable information or personal health information was compromised in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

**Tennessee Class:** All persons in Tennessee whose personally identifiable information or personal health information was compromised in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

119. Excluded from the Class are CHS, CHSPSC, LLC and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

120. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

121. The members of the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. CHSPSC reported to the Maine Attorney General that approximately 1,173,555 persons' information was exposed in the Data Breach.<sup>62</sup>

122. Common questions of law and fact exist as to all Class members and predominate

---

<sup>62</sup> See *Addendum to Previous Notification*, CSPSC (Apr. 17, 2023), available at <https://apps.web.maine.gov/online/aeviewer/ME/40/810b151b-febe-43ef-9b77-b4c8ea0d9f4d.shtml> (last accessed Apr. 26, 2023) (under "Notification and Protection Services" heading, click link titled "ME.pdf").

over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

- a. Whether either or both of the Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII/PHI from unauthorized access and disclosure;
- b. Whether either or both of the Defendants had duties not to disclose the PII/PHI of Plaintiffs and Class members to unauthorized third parties;
- c. Whether either or both of the Defendants failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII/PHI;
- d. Whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;
- e. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiffs and Class members;
- f. Whether Defendants breached their duties to protect Plaintiffs' and Class members' PII/PHI; and
- g. Whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

123. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

124. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by CHSPSC, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

125. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

126. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

## **CAUSES OF ACTION**

### **COUNT I**

#### **NEGLIGENCE**

**(Against Both Defendants on Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes)**

127. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.



128. Both Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding, securing, and protecting the PII/PHI in their possession, custody, or control. This duty extended to any vendor selected by Defendants to be entrusted with the sensitive data of Plaintiffs and Class Members.

129. Defendants knew or should have known the risks of collecting and storing Plaintiffs' and all other Class members' PII/PHI and the importance of maintaining and using secure systems. Defendants knew or should have known of the many data breaches that have targeted companies that stored PII/PHI in recent years—including their own in 2014.

130. Given the nature of Defendants' business, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified and foreseen that the third parties with whom they contract could have vulnerabilities in their systems and prevented the dissemination of Plaintiffs' and Class members' PII/PHI.

131. Indeed, CHS' last Form 10-K that it filed prior to the breach on October 27, 2022, identified the following risk factor that could materially impact the company's financial performance: "security breaches, cyber-attacks, loss of data, [and] other cybersecurity threats or incidents. . . ."

132. CHSPSC also makes explicit statements on its website that it is aware of the risk of potential data breaches, that it will follow privacy laws and regulations, and that it will use reasonable methods to protect the PII/PHI in its control.

133. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to ensure that the third parties that they share PII/PHI with design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures,

protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to them—including Plaintiffs’ and Class members’ PII/PHI.

134. Plaintiffs and Class members had no ability to protect their PII/PHI that was, or remains, in Defendants’ possession.

135. It was or should have been reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs’ and Class members’ PII/PHI by failing to ensure that the third parties that they share PII/PHI with design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs’ and Class members’ PII/PHI to unauthorized individuals.

136. But for Defendants’ negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII/PHI would not have been compromised. The PII/PHI of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants’ failure to exercise reasonable care in safeguarding, securing, and protecting such PII/PHI by, *inter alia*, ensuring that third parties they contract with and shares PII/PHI with adopt, implement, and maintain appropriate security measures.

137. As a result of Defendants’ above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts

attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) loss of value of their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

## **COUNT II**

### **NEGLIGENCE *PER SE***

**(Against Both Defendants on Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes)**

138. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

139. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

140. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as CHSPSC, of failing to employ reasonable measures to protect and secure PII/PHI.

141. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to ensure that third parties they contract with and shares PII/PHI with use reasonable measures to protect Plaintiffs' and all other Class members' PII/PHI and comply

with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI they obtain and store, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

142. Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence *per se*.

143. Plaintiffs and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

144. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

145. It was, or should have been, reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to ensure that the third-parties that they contract with and shares PII/PHI with design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

146. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA.

147. Plaintiffs and Class members have suffered and will suffer injury, including, but not limited: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated

with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; (vii) loss of value of their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

### **COUNT III**

#### **BREACH OF FIDUCIARY DUTY**

**(Against Both Defendants on Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes)**

148. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

149. As a condition of obtaining services or employment from Defendants, Plaintiffs and Class members gave Defendants their PII/PHI in confidence, believing that they would protect that information. Plaintiffs and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiffs' and Class members' PII/PHI created a fiduciary relationship between Defendants and Plaintiffs and Class members. In light of this relationship, Defendants must act primarily for the benefit of their and their affiliates' patients and employees, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

150. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. It breached that duty by failing to ensure that the third-parties they contract with and share PII/PHI with properly protect the integrity of the system containing Plaintiffs' and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class members' PII/PHI that they collected.

151. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; (vii) loss of value of their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

#### **COUNT IV**

##### **BREACH OF IMPLIED CONTRACT**

**(Against Both Defendants on Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes)**

152. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

153. In connection with receiving health care services or employment, Plaintiffs and all other Class members entered into implied contracts with Defendants.

154. Pursuant to these implied contracts, Plaintiffs and Class members benefited Defendants, directly or through an affiliate, through their labor or by paying monies to Defendants, and provided Defendants with their PII/PHI. In exchange, Defendants agreed to, among other things, and Plaintiffs understood that Defendants would: (1) provide products, services, or employment, to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI; (3) protect Plaintiffs' and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards; and (4) ensure third parties they contract with and provide PII/PHI to implement and maintain reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI.

155. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Defendants, on the other hand. Indeed, as set forth *supra*, Defendants recognized the importance of data security and the privacy of their and their affiliates' patients' and employees' PII/PHI. Had Plaintiffs and Class members known that Defendants would not adequately protect their PII/PHI, would not have paid for products or services or obtained employment from Defendants.

156. Plaintiffs and Class members performed their obligations under the implied contract when they provided Defendants with their PII/PHI and paid for products and services from Defendants or their affiliates, or completed work for Defendants or their affiliates, expecting that their PII/PHI would be protected.

157. Defendants breached their obligations under their implied contracts with Plaintiffs and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, and in failing to ensure that third parties they contract with and share PII/PHI with implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

158. Defendants' breach of their obligations of the implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the resulting injuries to Plaintiffs and Class members.

159. Plaintiffs and all other Class members were damaged by Defendants' breach of implied contracts because: (i) they paid monies (directly or through their insurers or Defendants affiliates) or provided labor in exchange for data security protection they did not receive; (ii) they now face a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.



## **COUNT V**

### **BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND CLASS MEMBERS WERE INTENDED THIRD PARTY BENEFICIARIES (Against Both Defendants on Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes)**

160. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein. This claim is pleaded in the alternative to the breach of implied contract claim and unjust enrichment claim.

161. Plaintiffs bring this claim individually and on behalf of the Class.

162. Defendants had valid contracts with each of the hospitals and clinics. A principal purpose of those contracts was to securely store, transmit, and safeguard the PII/PHI of Plaintiffs and Class members.

163. Upon information and belief, Defendants and each of the contracting hospitals and clinics expressed an intention that Plaintiffs and Class members were intended third party beneficiaries of these agreements.

164. Plaintiffs and Class members are also intended third party beneficiaries of these agreements because recognizing them as such is appropriate to effectuate the intentions of the parties, and the circumstances indicate that Defendants intended to give the beneficiaries the benefit of the promised performance.

165. Defendants breached their agreements with the contracting hospitals and clinics by allowing the data breach to occur, and as otherwise set forth herein.

166. Defendants' breach caused foreseeable and material damages to Plaintiffs and class members.

## **COUNT VI**

### **UNJUST ENRICHMENT**

**(Against Both Defendants on Behalf of the Nationwide Class or, Alternatively, on Behalf of the Alabama, Florida, Mississippi, Pennsylvania and Tennessee Classes)**

167. Plaintiffs reallege and incorporate by reference the preceding paragraphs.

168. This claim is pleaded in the alternative to the breach of implied contract claim and intended third party beneficiary claim.

169. In obtaining services or employment from Defendants, Plaintiffs and Class members provided and entrusted their PII and PHI to them.

170. Plaintiffs and Class members conferred a monetary benefit upon Defendants in the form of monies paid for products or services or via the value of their labor (including by facilitating payments to Defendants), with an implicit understanding that Defendants would use some of their revenue to protect the PII/PHI they collect.

171. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members. Defendants benefitted from the receipt of Plaintiffs' and Class members' PII/PHI, as this was used to facilitate billing and payment services, as well as from Plaintiffs' and Class members' labor, which enabled Defendants to carry out their business.

172. As a result of Defendants' conduct, Plaintiffs and Class members suffered actual damages.

173. Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendants failed to adequately implement the data privacy and security procedures for itself and the third parties that they contract with and share PII/PHI with that Plaintiffs and Class members paid for and expected, and that were otherwise mandated by federal, state, and local laws and industry standards.

174. Defendants should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds they received as a result of the conduct and Data Breach alleged herein.

## **COUNT VII**

### **VIOLATIONS OF ALABAMA DECEPTIVE TRADE PRACTICES ACT Ala. Code § 8-19-1, *et seq.* (Against Both Defendants on Behalf of the Alabama Class)**

175. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

176. The Alabama Deceptive Trade Practices Act (“ADTPA”) was created to protect Alabama consumers from fraudulent or deceptive business practices.

177. Plaintiff Angela Martin (“Alabama Plaintiff”) and Alabama Class members obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants.

178. As set forth more fully above, Defendants caused injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of highly sensitive PII/PHI; deprivation of the value of PII/PHI; and overpayment for services that did not include adequate data security.

179. Defendants failed to disclose the breach for nearly two months and breached their duties and obligations to remedy the inadequate security and protect their customers whose PII/PHI was exposed.

180. Defendants conduct constituted, among other things, the following prohibited fraudulent, deceptive, unconscionable, and unfair business practices: (a) engaging in fraudulent, deceptive, unconscionable, and unfair conduct that creates a likelihood of confusion and

misunderstanding; and (b) engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

181. Defendants conduct was deceptive because the omissions created a likelihood of confusion and misunderstanding and had the capacity or tendency to deceive and, in fact, did deceive, ordinary consumers, including Alabama Plaintiff. Knowledge of those facts would have been a substantial factor in Alabama Plaintiff's, as well as Alabama Class members', decision to take steps to protect their PII/PHI and to protect themselves from identity theft.

182. Defendants owed Alabama Plaintiff and Alabama Class members, among others, a duty to disclose these facts because they were known and/or accessible exclusively to Defendants who had exclusive and superior knowledge of the facts; because the facts would be material to reasonable consumers; because Defendants actively concealed them and because Defendants intended for customers to rely on the safety of their PII/PHI.

183. Alabama Plaintiff and members of the Alabama Class justifiably relied on the material representations and/or omissions by Defendants, and reasonable consumers would have been expected to rely upon these omissions, in part, because they are omissions that impact PII/PHI.

184. Defendants conduct actually and proximately caused an actual ascertainable loss of money or property to Alabama Plaintiffs (as set forth above) and members of the Alabama Class. Absent Defendants unfair, deceptive, fraudulent and/or unconscionable conduct, Alabama Plaintiff and Alabama Class members would have behaved differently and would not have provided their PHI or PII to Defendants.

185. Accordingly, pursuant to Ala. Code § 8-19-10(a)(1), Alabama Plaintiff and Alabama Class members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence.

### **COUNT VIII**

#### **VIOLATIONS OF MISSISSIPPI DECEPTIVE TRADE PRACTICES ACT Miss. Code § 75-24-1, *et seq.* (Against Both Defendants on Behalf of the Mississippi Class)**

186. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

187. The Mississippi Consumer Protection Act was created to protect Mississippi consumers from unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce.

188. Plaintiffs Lola Tatum, Brandy McGowen, and Richard Walck (“Mississippi Plaintiffs”) and Mississippi Class members obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants.

189. As set forth more fully above, Defendants caused injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of highly sensitive PII/PHI; deprivation of the value of PII/PHI; and overpayment for services that did not include adequate data security.

190. Defendants concealed and failed to disclose the breach for nearly two months, and in doing so, breached their duties and obligations to remedy the inadequate security and protect their customers whose PII/PHI was exposed.

191. Defendants conduct described herein constitutes the act, use or employment of deception, false promise, misrepresentation, unfair practice and the concealment, suppression, and

omission of material facts in connection with Data Breach in Mississippi, made with the intention that Plaintiff and Mississippi Class members would rely on the safety of their PII/PHI, making it unlawful under Miss. Code § 75-24-1, *et seq.*

192. Defendants' conduct constituted, among other things, the following unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce: (a) causing a probability of confusion or misunderstanding as to the source, sponsorship, approval, or certification of goods or services; (b) representing that goods or services are of a particular standard, quality, or grade; (c) advertising or representing goods or services with intent not to dispose of those goods or services as advertised or represented; (d) failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer; (e) making a representation of fact or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is; and (f) failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

193. Defendants' conduct was unfair, unconscionable, or deceptive because the omissions created a likelihood of confusion and misunderstanding and had the capacity or tendency to deceive and, in fact, did deceive, ordinary consumers, including Mississippi Plaintiffs. Knowledge of those facts would have been a substantial factor in Mississippi Plaintiffs', as well as Mississippi Class members', decision to rely on the safety of their PII/PHI.

194. Defendants owed Mississippi Plaintiffs and Mississippi Class members, among others, a duty to disclose these facts because they were known and/or accessible exclusively to Defendants who had exclusive and superior knowledge of the facts; because the facts would be

material to reasonable consumers; because Defendants actively concealed them and because Defendants intended for consumers to rely on the safety of their PII/PHI.

195. Mississippi Plaintiffs and members of the Mississippi Class justifiably relied on the material misrepresentations and/or omissions by Defendants, and reasonable consumers would have been expected to rely upon these representations and/or omissions, in part, because they are representations and/or omissions that impact decision to take steps to protect their PII/PHI and to protect themselves from identity theft.

196. Accordingly, pursuant to Miss. Code § 75-24-1, *et seq.*, Mississippi Plaintiffs and Mississippi Class members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Mississippi Plaintiffs and Mississippi Class members are also entitled to all available statutory, exemplary, treble, and/or punitive damages and attorneys' fees based on the amount of time reasonably expended and equitable relief necessary or proper to protect them from Defendants unlawful conduct.

### **COUNT IX**

#### **VIOLATIONS OF PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW**

**73 Pa. Stat. Ann. § 201-1, *et seq.***

**(Against Both Defendants on Behalf of the Pennsylvania Class)**

197. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

198. The Pennsylvania Unfair Trade Practices and Consumer Protection Law was created to protect Pennsylvania consumers from fraudulent or deceptive business practices.

199. Plaintiff Kelly Kern (“Pennsylvania Plaintiff”) and Pennsylvania Class members obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants.

200. As set forth more fully above, Defendants caused injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of highly sensitive PII/PHI; deprivation of the value of PII/PHI; and overpayment for services that did not include adequate data security.

201. Defendants concealed and failed to disclose the breach for nearly two months, and in doing so, breached their duties and obligations to remedy the inadequate security and protect their customers whose PII/PHI was exposed.

202. Defendants concealed and failed to disclose that they lacked sufficient measures in place to safeguard the sensitive data entrusted to them (and which they entrusted to a vendor).

203. Defendants conduct was fraudulent and deceptive because the omissions created a likelihood of confusion and misunderstanding and had the capacity or tendency to deceive and, in fact, did deceive, ordinary consumers, including Pennsylvania Plaintiff. Ordinary consumers, including Pennsylvania Plaintiff, would have found it material to their healthcare or employment decisions that Defendants lacked adequate security measures to adequately safeguard their PII/PHI. Knowledge of those facts would have been a substantial factor in Pennsylvania Plaintiffs’, as well as other Pennsylvania Class members’, decision to obtain services or provide labor to Defendants.

204. Defendants owed Pennsylvania Plaintiff and Pennsylvania Class members, among others, a duty to disclose these facts because they were known and/or accessible exclusively to Defendants who had exclusive and superior knowledge of the facts; because the facts would be



material to reasonable consumers; because Defendants actively concealed them and because Defendants intended for consumers to rely on the omissions in question.

205. Pennsylvania Plaintiffs, and members of the Pennsylvania Class, justifiably relied on the material misrepresentations and/or omissions by Defendants, and reasonable consumers would have been expected to rely upon these omissions, in part, because they are omissions that impact seriously on a consumer's PII/PHI.

206. Accordingly, pursuant to the 73 Pa. Stat. Ann. § 201-1, *et seq.*, Pennsylvania Plaintiff and Pennsylvania Class members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Pennsylvania Plaintiff and Pennsylvania Class members are also entitled to recover all available statutory, exemplary, treble, and/or punitive damages, costs of suit, and attorneys' fees based on the amount of time reasonable expended and equitable relief necessary, and all such other relief as the Court deems proper.

### **COUNT X**

#### **VIOLATIONS OF TENNESSEE CONSUMER PROTECTION ACT Tenn. Code Ann. § 47-18-101, *et seq.* (Against Both Defendants on Behalf of the Tennessee Class)**

207. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

208. The Tennessee Consumer Protection Act ("TCPA") was created to protect Tennessee consumers from fraudulent or deceptive business practices.

209. Plaintiff Sandra Kuffrey and Plaintiff Wilhelmina Gill ("Tennessee Plaintiffs"), Tennessee Class members, and Defendants are persons under the TCPA.

210. Tennessee Plaintiffs and Tennessee Class members obtained healthcare or related services from hospitals or clinics serviced by or affiliated with Defendants.

211. As set forth more fully above, Defendants caused injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of highly sensitive PII/PHI; deprivation of the value of PII/PHI; and overpayment for services that did not include adequate data security.

212. Defendants concealed and failed to disclose the breach for nearly two months, and in doing so, breached their duties and obligations to remedy the inadequate security and protect their customers whose PII/PHI was exposed.

213. Defendants concealed and failed to disclose in any of their marketing materials, advertising, packaging, and/or any other communication that they lacked sufficient measures in place to safeguard the sensitive data entrusted to them (and which they entrusted to a vendor).

214. Defendants conduct constitutes “[u]nfair or deceptive acts or practices affecting the conduct of any trade or commerce” in Tennessee, making it unlawful under Tenn. Code Ann. § 47-18-104(a).

215. Under the circumstances herein, Defendants’ failure to disclose that they lacked sufficient and reasonable data security protections constituted fraudulent, deceptive, and unfair business practices.

216. Defendants conduct was fraudulent and deceptive because the omissions created a likelihood of confusion and misunderstanding and had the capacity or tendency to deceive and, in fact, did deceive, ordinary consumers, including Tennessee Plaintiffs and Tennessee Class members. Ordinary consumers, including Tennessee Plaintiffs and Tennessee Class members,

would have found it material to their conduct had they known that Defendants lacked sufficient data security measures.

217. Defendants owed Tennessee Plaintiffs and Tennessee Class members a duty to disclose these facts because they were known and/or accessible exclusively to Defendants who had exclusive and superior knowledge of the facts; because the facts would be material to reasonable consumers; because Defendants actively concealed them and because Defendants intended for consumers to rely on the omissions in question.

218. Tennessee Plaintiffs and members of the Tennessee Class justifiably relied on the material misrepresentations and/or omissions by Defendants, and reasonable consumers would have been expected to rely upon these omissions, in part, because they are omissions that impact seriously on a consumer's PII/PHI.

219. Defendants' conduct actually and proximately caused an ascertainable loss of money or property to the Tennessee Plaintiffs (as set forth above) and members of the Tennessee Class. Absent Defendants' unfair, deceptive, and/or fraudulent conduct, Tennessee Plaintiffs and Tennessee Class members would have behaved differently and would not have entrusted their most sensitive PII and PHI to Defendants.

220. Accordingly, pursuant to the aforementioned statutes, Tennessee Plaintiffs and Tennessee Class members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Tennessee Plaintiffs and Tennessee Class members are also entitled to recover all available statutory, exemplary, treble, and/or punitive damages, costs of suit, and attorneys' fees based on the amount of time reasonable expended and equitable relief necessary, and all such other relief as the Court deems proper.

### **PRAYER FOR RELIEF**

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendants from experiencing yet another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

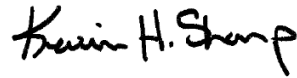
F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

### **JURY TRIAL DEMANDED**

Plaintiffs demand a trial by jury of all claims in this Consolidated Amended Class Action Complaint so triable.

Dated: June 15, 2023

Respectfully submitted,



---

Kevin H. Sharp, BPR No. 016287  
Leigh Anne St. Charles, BPR No. 036945  
Jonathan Tepe, BPR No. 037266  
**SANFORD HEISLER SHARP, LLP**  
611 Commerce Street, Suite 3100  
Nashville, TN 37203  
Telephone: (615) 434-7000  
Facsimile: (615) 434-7020  
ksharp@sanfordheisler.com  
lstcharles@sanfordheisler.com  
jtepe@sanfordheisler.com

**SHUB & JOHNS LLC**

Benjamin F. Johns (admitted *pro hac vice*)  
Samantha E. Holbrook (admitted *pro hac*)  
Four Tower Bridge  
200 Barr Harbor Drive, Suite 400  
Conshohocken, PA 19428  
(610) 477-8380  
bjohns@shublawyers.com  
sholbrook@shublawyers.com

**BARNOW AND ASSOCIATES, P.C.**

Ben Barnow (admitted *pro hac vice*)  
Anthony L. Parkhill (admitted *pro hac vice*)  
Riley W. Prince (admitted *pro hac vice*)  
205 West Randolph Street, Ste. 1630  
Chicago, IL 60606  
Tel: 312-621-2000  
Fax: 312-641-5504  
b.barnow@barnowlaw.com  
aparkhill@barnowlaw.com  
rprince@barnowlaw.com

**BAILEY GLASSER LLP**

Bart D. Cohen (admitted *pro hac vice*)  
1622 Locust Street  
Philadelphia, PA 19103

(215) 274-9420  
bcohen@baileyglasser.com

*Interim Co-Lead Class Counsel*

**HERZFELD, SUETHOLZ, GASTEL,  
LENISKI AND WALL, PLLC**

Benjamin A. Gastel (BPR #28699)  
223 Rosa L. Parks Avenue, Suite 300  
Nashville, Tennessee 37203  
(615) 800-6225  
ben@hsglawgroup.com

*Additional Plaintiffs' Counsel*

### **CERTIFICATE OF SERVICE**

I, Kevin H. Sharp, hereby certify that the foregoing Consolidated Amended Class Action Complaint was filed on this 15th day of June 2023 using the Court's CM/ECF System, thereby serving it upon all counsel of record in these consolidated proceedings with the exception of Marcio W. Valladares, who was served via electronic and/or first-class mail.

Jonathan O. Harris  
Jackson Lewis P.C. (Nashville Office)  
611 Commerce Street, Suite 3102  
Nashville, TN 37203  
jonathan.harris@jacksonlewis.com

Jackson E. Biesecker  
Jackson Lewis LLP  
6100 Oak Tree Boulevard, Suite 400  
Cleveland, OH 44131  
(216) 750- 0404  
jackson.biesecker@jacksonlewis.com

Bart D. Cohen  
Bailey Glasser LLP  
1622 Locust Street  
Philadelphia, PA 19103  
304-345-6555  
Fax: 304-342-1110  
bcohen@baileyglasser.com

Benjamin A. Gastel  
Herzfeld, Suetholz, Gastel, Leniski and Wall, PLLC  
223 Rosa L Parks Ave., Ste 300  
Nashville, TN 37203  
615-800-6225  
ben@hsglawgroup.com

Benjamin F. Johns  
Shub & Johns LLC  
Four Tour Bridge  
200 Barr Harbor Drive, Suite 400  
West Conshohocken, PA 19428  
(610) 477-8380  
bjohns@shublawayers.com

Samantha E. Holbrook  
Shub & Johns LLC  
Four Tour Bridge  
200 Barr Harbor Drive, Suite 400  
West Conshohocken, PA 19428  
(610) 477-8380  
sholbrook@shublawyers.com

Cody Galaher , I  
Galaher Law, PLLC  
725 Cool Springs Blvd. Suite #600  
Franklin, TN 37067  
(615) 732-6168  
CGalaher@ForThePeople.com

Laura Grace Van Note  
Cole & Van Note  
555 12th Street, Suite 1725  
Oakland, CA 94607  
(510) 891-9800  
lvn@colevannote.com

Kevin Laukaitis  
Laukaitis Law Firm LLC  
737 Bainbridge St #155  
Philadelphia, PA 19147  
(215) 789-4462  
klaukaitis@laukaitislaw.com

Seamus T. Kelly  
Music City Law, PLLC  
1033 Demonbreun Street, Suite 300  
Nashville, TN 37203  
(615) 200-0682  
seamus@musiccityfirm.com

Spencer Sheehan  
Sheehan & Associates, P.C.  
60 Cuttermill Road, Suite 412  
Great Neck, NY 11021  
516-268-7080  
Fax: 516-234-7800  
spencer@spencersheehan.com

Anthony Parkhill  
Barnow and Associates, P.C.



205 West Randolph Street, Suite 1630  
Chicago, IL 60606  
(312) 621-2000  
Fax: (312) 641-5504  
aparkhill@barnowlaw.com

Ben Barnow  
Barnow and Associates, P.C.  
205 West Randolph Street, Suite 1630  
Chicago, IL 60606  
(312) 621-2000  
Fax: (312) 641-5504  
b.barnow@barnowlaw.com

Leigh Anne St. Charles  
Sanford Heisler Sharp, LLP  
611 Commerce Street, Suite 3100  
Nashville, TN 37203  
(615) 434-7006  
Fax: (615) 434-7020  
lstcharles@sanfordheisler.com

Jonathan Tepe  
Sanford Heisler Sharp, LLP  
611 Commerce Street, Suite 3100  
Nashville, TN 37203  
615-434-7002  
Fax: 615-434-7020  
jtepe@sanfordheisler.com

Riley W. Prince  
Barnow and Associates, P.C.  
205 West Randolph Street, Suite 1630  
Chicago, IL 60606  
(312) 621-2000  
Fax: (312) 641-5504  
rprince@barnowlaw.com

David A. McLaughlin  
901Attorneys, LLC  
200 Jefferson Avenue, Suite 900  
Memphis, TN 38103  
901-671-1551  
Fax: 901-671-1571  
david@901attorneys.com

Gary F. Lynch  
Lynch Carpenter, LLP  
1133 Penn Avenue, 5th Floor  
Pittsburgh, PA 15222  
412-322-9243  
gary@lcllp.com

James J. Pizzirusso  
Hausfeld LLP  
888 16th Street, NW, Suite 300  
Washington, DC 20006  
(202) 540-7200  
jpizzirusso@hausfeld.com

Nicholas A. Colella  
Lynch Carpenter LLP  
1133 Penn Avenue, 5th Floor  
Pittsburgh, PA 15222  
(412) 322-9243  
Fax: (412) 231-0246  
nickc@lcllp.com

Steven M. Nathan  
Hausfeld LLP  
33 Whitehall Street, 14th Floor  
New York, NY 1100  
(646) 357-1100  
snathan@hausfeld.com

Alyson S. Beridon  
Herzfeld, Suetholz, Gastel, Leniski and Wall, PLLC  
425 Walnut St., Ste 2315  
Cincinnati, OH 45202  
513-381-2224  
Fax: 615-255-5419  
alyson@hsglawgroup.com

John A. Yanchunis  
Morgan & Morgan (Tampa Office)  
201 N Franklin Street, 7th Floor  
Tampa, FL 33602  
(813) 223-5505  
Fax: (813) 223-5402  
jyanchunis@forthepeople.com

Marcio W. Valladares  
Complex Litigation Group  
201 North Franklin Street, 7th Floor  
Tampa, FL 33602  
(813) 223-5505  
mvalladares@forthepeople.com

Ra O. Amen  
Complex Litigation Group  
201 North Franklin Street, 7th Floor  
Tampa, FL 33602  
(813) 223-5505  
RAmen@forthepeople.com

Robert B. Keaty , II  
Morgan & Morgan (Nashville Office)  
810 Broadway  
Suite 105  
Nashville, TN 37203  
(615) 928-9901  
bkeaty@forthepeople.com

/s/ Kevin H. Sharp  
Kevin H. Sharp